AMENDMENTS TO THE SPECIFICATION:

Please add the following new paragraph after paragraph [0003] (i.e., the last paragraph), on page 3:

Another exemplary embodiment of the present invention involves a method for generating, personalizing, and certifying an asymmetrical cryptokey in accordance with one of an operation performed at a central, secure location corresponding to a trust center and an operation performed at a user location in cooperation with the trust center using a secure transmission between a user and the trust center. This method, shown in Fig. 1, includes causing 1 the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair. Further, at least one encryption key pair is produced 2, the encryption key pair including a public part and a secret part. The public part of the encryption key pair is marked 3 using an assigned secret part of the previously generated signature key pair. After the public part is marked, then the encryption key pair is transmitted 4 to the trust center. The encryption key pair is unequivocally assigned 5 to the user. The trust center is caused 6 to check the unequivocal assignment of the encryption key pair by using a public part of the previously generated signature key pair. After the check of the unequivocal assignment is performed successfully, the trust center is caused 7 to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair. The new certificate is encrypted 8 using the public part of the at least one encryption key pair. The trust center is caused 9 to transmit the encrypted new certificate to the user.